Man In The Middle

Pablo Parra Garófano

-Descripción general.

-Subataques.

-Ataque real a un banco.

-¿Por qué https?.

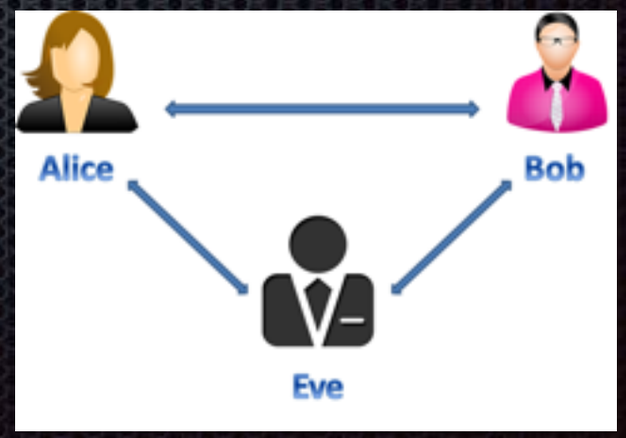
-Herramienta para MITM: Ettercap.

-Demo.

Descripción:

Un ataque de intermediario (MITM), consiste:

Introducirse en una red entre dos equipos finales y hacer que todo el tráfico pase por el atacante de forma que este pueda acceder a los mensajes que se envían, desencriptar, insertar o incluso modificar los mensajes que se envían.



Subataques:

-Interceptación de la comunicación.

-Ataques de sustitución (Spoofing).

-Ataques de reinyección.

-Ataques de denegación de servicio (DoS).

Ataque real:

- Banco de Absa (África).
- 49 personas arrestadas.
- 6.000.000 € en un tiempo muy corto.

- Detección de correos electrónicos y solicitudes de pago.
- Enviaban correos falsos con enlaces para que iniciaran sesión en una página recreada a la perfección.

¿Por qué HTTPS?

Hyper Text Transport Protocol Secure

Combinación de HTTP y SSL/TLS (Secure Sockets Layer / Transmission Layer Security).

Nos proporciona:

- Encriptación.

- Integridad de los datos.

- Autenticación.

Interceptor/Sniffer para principalmente envenenamiento ARP de la máquina objetivo, de forma que seamos la puerta de enlace entre el objetivo y el servidor al que quiere acceder.

Demo